



FortiAnalyzer

Version 5.4

QuickStart Guide

REGISTER FOR SUPPORT

への防御

请马上注册

点信息、最新威胁防护

您的飞塔产品

登録のお願い

登録すると次のメリットがあります。

本日、フォーティネット製品の登録をしてください。

テクニカルサポート・新機能の追加・新しい脅威

您在注册以后才能得到技术支持、新产品特

REGISTER YOUR FORTINET PRODUCT TO RECEIVE:

- Technical Support
- New product features
- Protection from new threats

LA REISTRAZIONE TI PERMETTE DI USUFRUIRE DI:

Supporto Tecnico

- Nuove funzionalita
- Proteezione dalle ultime minaccce

VOUS DEVEZ ENREGISTRER LE PRODUIT POUR RECEVOIR:

SUPPORT

Support technique

Toll free: 1 866 648 4638 Phone: 1 408 486 7899

http://forti.net/support

Fax: 1 408 235 7737

DEBE REGISTRAR EL PRODUCTO PARA RECIBIR:

Nouvelles fonctionnalitées du produit

Protection contre de nouvelles menaces.

- Apoyo técnico
- Nuevas funcionalidades del producto
- Protección contra ataques

November 03, 2016 OS-541-370731-20160513

Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiGate® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

EC DAY1: SETUP

- Configure network settings and admin account
- Set up FortiGate to send logs
- View logs from Log View



Configure FortiAnalyzer Network Settings

1. Connect the FortiAnalyzer **Port 1** to the **Management computer port**.



- Set the management computer to be on the same subnet as FortiAnalyzer. (The default is 192.168.1.99.)
 For Example: IP Address: 192.168.1.10
 Netmask: 255.255.255.0
- 3. Visit https://192.168.1.99 in your web browser.
- 4. Log in with username **admin** and no password.



Configure FortiAnalyzer Network Settings

- 1. Go to System Settings > Network.
- 2. Change the IP address/Netmask to your internal network.
- 3. Keep the default Administrative Access settings.
- 4. Specify a **Default Gateway**.
- 5. Change the IP address/Netmask of the management computer accordingly to reconnect it to FortiAnalyzer.

IP Address/Netmask	10.3.112.95/255.255.0.0
IPv6 Address	::/0
Administrative Access	☑ HTTPS ☑ HTTP ☑ PING ☑ SSH ☑ TELNET □ SNMP □ Web Service □ Aggregator □ FortiMana
IPv6 Administrative Access	☑ HTTPS ☑ HTTP ☑ PING ☑ SSH ☑ TELNET □ SNMP □ Web Service □ Aggregator □ FortiMana
Default Gateway	172.16.96.1
Primary DNS Server	172.16.100.100
Secondary DNS Server	172.16.100.80

Set Up Administrator Accounts

- Go to System Settings > Admin > Administrator, and click Create New in the toolbar.
- 2. Enter user name and password.
- 3. Click **OK** to save the change.

Jser Name	admin_John
Comments	
	0/127
dmin Type	LOCAL
lew Password	• • • • •
Confirm Password	• • • • •
dmin Profile	Super_User *
dministrative Domain	All ADOMs All ADOMs except specified ones Specify
rusted Hosts	OFF
Iser Information >	
	OK Cancel



Configure Log Storage Policy

- 1. Go to System Settings > Dashboard.
- 2. In the System Information widget, under Log Storage Policy, select Edit Log Storage policy.
 - Data Policy:
 - Set Keep Logs for Analytics to 90 days.
 - Set Keep Logs for Archive to 180 days.

• Disk Utilization:

Keep the default values.

ata Policy						
Keep Logs for Analytics	60		Days	٣		
Keep Logs for Archive	365		Days	٣		
sk Utilization						
Maximum Allowed	1000		MB	٣	Out of Available: 63.	6 GB
Analytics : Archive	70%	Ŧ	30%		Modify	
Alert and Delete When Usage Reaches	90%	•				
analytic or archive log upages evened the	configured dick a	uota hofor	the retention	poriod ove	iros the eldest leas wil	I be deleted
analytic or archive log usages exceed the	configured disk q	uota before	e the retention	period exp	ires, the oldest logs wil	l be deleted.

You can monitor the log storage settings and adjust as you go.

Check License and Registration



Check that you have a valid license for the IOC Service, to enable the feature.



2 Connect FortiGate to FortiAnalyzer



Configure FortiGate Log Settings

- 1. Log in to the FortiGate GUI from the management computer.
- 2. Go to Log & Report > Log Settings.
 - Turn on Send Logs to FortiAnalyzer/FortiManager.
 - Enter the IP address of the FortiAnalyzer and click Apply.

172.16.96.5	Test Connectivity
Store & Upload Logs Realtime	•
	T72.16.96.5 Store & Upload Logs Realtime



Don't click **Test Connectivity** yet. You need to register this FortiGate on the FortiAnalyzer first.



Register FortiGate on FortiAnalyzer

1. Go to **Device Manager** of FortiAnalyzer. Click the **Unregistered Devices** tab in the quick status bar.



- 2. Select the FortiGate device, and click Add.
- 3. In the Add Device dialog box that opens, select the root ADOM, type a device name, and click **OK**.

Device Mana	ger \sim						٩	admin 🗸		ę
	O Devices Total	?	1 Devices Unregistered		O Devices Log Status Down	e	0	X Storage U Total 19.5 GB	sed	
+ Add 🕆 Delete	2								(0
Device Name		N	4odel		Serial Number	Co	nnecting IP			
FG30DP3X130	00036	F	ortiGate-30D-POE		FG30DP3X13000036	17	2.172.2.17			
	_									
	Add Device									
	Add the following device(s) to ADOM:	Corporate			×				
	Device Name	Assign New D	Device Name							
	FG30DP3X13000036	FG30DP								
					ок		Cancel			
		_		_		_	_	_		
										1

Test Connectivity on FortiGate

1. Go back to the Log Settings pane of FortiGate, and click **Test Connectivity**. If the connection is successfully established, a connection summary is shown.



Verify Logs Being Received

1. Go to Log View do of the FortiAnalyzer. Select Last 5 minutes from the time period list and press **GO**. You should be able to see the FortiGate logs.

	Add	Column Settings	🛢 Column Settings 🗸 🛛 🗲 Tools 🗸								
lli Event >	#	▼Date/Time	Device ID	Action	Source	Destination IP	Service	Sent/Received	User	Application	Security Event L
Security >	1	14:27:26	FG100D3G0000291	1	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.3 KB		Web Management	
♥ VolP	2	14:27:25	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 B		Web Management	
a (0)	3	14:27:25	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	2.3 KB/2.9 KB		Web Management	
& Custom View	4	14:27:20	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	4.3 KB/4.5 KB		Web Management	
Storage Statistics	5	14:27:20	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 B		Web Management	
Log Browse	6	14:27:16	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.8 KB		Web Management	
III Los Group	7	14:27:14	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 B		Web Management	
El cop oroup	8	14:27:11	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.3 KB/1.2 KB		Web Management	
	9	14:27:07	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 B		Web Management	
	10	14:27:06	FG100D3G0000291	 Image: A second s	172.18.27.180	172.18.27.206	HTTP	1.3 KB/1.2 KB		Web Management	
	11	14:27:04	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.8 KB		Web Management	
	12	14:27:01	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 B		Web Management	
	13	14:27:00	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.3 KB/1.3 KB		Web Management	
	14	14:27:00	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	3.3 KB/3.0 KB		Web Management	
	15	14:26:56	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	2.3 KB/2.9 KB		Web Management	
	16	14:26:55	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 B		Web Management	
	17	14:26:51	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.3 KB/1.3 KB		Web Management	
	18	14:26:49	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	3.4 KB/2.7 KB		Web Management	
	19	14:26:46	FG100D3G0000291	×	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 B		Web Management	
	20	14:26:46	FG100D3G0000291	×	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.8 KB		Web Management	
	21	14:26:39	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	13.7 KB/33.8		Web Management	
	22	14:26:39	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	2.2 KB/4.8 KB		Web Management	
	23	14:26:31	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	3.0 KB/6.9 KB		Web Management	
	24	14:26:31	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	4.3 KB/10.0 KB		Web Management	
	25	14:26:31	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	4.2 KB/11.2 KB		Web Management	
	26	14:26:29	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	5.4 KB/26.2 KB		Web Management	
	27	14:26:26	FG100D3G0000291	×	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.2 KB		Web Management	
	28	14:26:19	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.0 KB		Web Management	
	29	14:26:16	FG100D3G0000291	× -	fe80::20c:29ff:febd:614e	ff02::16	icmp6/143/0	876.0 B/0.0 KB		icmp6/143/0	
	30	14:26:16	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.0 KB		Web Management	
	31	14:26:16	FG100D3G0000291	~	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.0 KB		Web Management	
	32	14:26:09	FG100D3G0000291	~		ff02::16	icmp6/143/0	3.0 KB/0.0 KB		icmp6/143/0	
	33	14:26:01	FG100D3G0000291	~	fe80::20c:29ff:fee3:39c7	ff02::16	icmn6/143/0	572.0 B/0.0 KB		icmn6/143/0	

DAY 2: NAVIGATE

- Interact with FortiView
- Generate reports
- Monitor events

1 Look into FortiView Summaries

In FortiView, the Summary view provides different Fortinet summaries as widgets. You can customize the widgets being displayed, and also drill down into each widget for further info.

Fortiview Summary



ĒØ 11

Top Threats

Drill Down Sort Entries Double-click Click a column the entry. heading. :

FortiView 🗸						ADOM: root	요 admin 🗸 🍵			
E Summary	Add Filter			🔃 💻 All Devices 👻 🕓 Last 1 Hour 👻 😡						
Threats	Threat	Category	Threat Level	▼Threat Score(■ Blocked/ ■ Allowed)	Incidents(Blocked/ Allow	red)				
	blocked-connection 2	Blocked by Firewall Policy	Critical	5,251,860	175,062					
Threat Man	Proxy.HTTP	Proxy	High	2,807,590	56,157					
100	blocked-connection	Blocked by Firewall Policy	High	800,790	26,693					
	C Zeroaccess.Botnet	Botnet	Critical	592,900	5,929					
Traffic	Failed Connection Attempts to 208.91.113.179	Failed Connection Attempts	Low	375,205	75,041					
# Applications & Websites	Failed Connection Attempts to 172.16.100.80	Failed Connection Attempts	Low	259,635 🥌	51,927					
A VPN	> Failed Connection Attempts to 172.16.100.80	Failed Connection Attempts	Medium	191,400 🧧	38,280					
⊗ WiFi	Failed Connection Attempts to 8.8.8.8	Failed Connection Attempts	Low	115,690 -	23,138					
* *****	Failed Connection Attempts to 172.16.100.100	Failed Connection Attempts	Low	109,435 -	21,887					
System	Failed Connection Attempts to 192.175.48.42	Failed Connection Attempts	Low	79,185	15,837	Add Filter	10	0 A AI	Devices + 🙁 Last 1 Hour + 🛛 😡	B
EndPoints	Failed Connection Attempts to 208.91.113.241	Failed Connection Attempts	Low	74,130	14,826					Thread Course
	Failed Connection Attempts to 8.8.8.8	Failed Connection Attempts	Medium	71,650	14,330					ort By Threat Score *
	Failed Connection Attempts to 192.175.48.6	Failed Connection Attempts	Low	67,850	13,570					Threat Score
	Failed Connection Attempts to 172.16.100.100	Failed Connection Attempts	Medium	60,620	12,124					Incidents
	Failed Connection Attempts to 208.91.113.206	Failed Connection Attempts	Low	51,835	10,367 💶					
	Failed Connection Attempts to 208.91.113.104	Failed Connection Attempts	Low	50,895	10,179					
	OpenVPN	Proxy	High	46,440	1,526			Your.Fr., Failed		
	Failed Connection Attempts to 172.16.86.107	Failed Connection Attempts	Medium	44,690	8,938 💻			Failed Failed		
	Failed Connection Attempts to 208.91.113.201	Failed Connection Attempts	Low	41,350	8,270 🔲				Failed	
	Failed Connection Attempts to 208.91.112.53	Failed Connection Attempts	Medium	40,630	8,126			Failed	Failed	
	Failed Connection Attempts to 172.16.86.91	Failed Connection Attempts	Medium	38,450	7,690		Failed	Zeroaccess.Botne	Failed	
	Failed Connection Attempts to 208.91.113.101	Failed Connection Attempts	Low	36,890	7,378 📟			Falled Connec		
	Failed Connection Attempts to 208.91.113.122	Failed Connection Attempts	Low	33,005	6,601 🗖		Falled		Failed	
	Failed Connection Attempts to 172.16.86.104	Failed Connection Attempts	Medium	30,960	6,192		Faile	ed Conn		
	Failed Connection Attempts to 192.168.224.161	Failed Connection Attempts	Low	29,315	5,863 📮		Failed		Failed	
	Failed Connection Attempts to 172.16.86.241	Failed Connection Attempts	Medium	27,805	5,561					Naled
	Failed Connection Attempts to 172.16.96.86	Failed Connection Attempts	Medium	27,140	5,428					Falled
	Failed Connection Attempts to 192.168.224.162	Failed Connection Attempts	Low	26,295	5,259		Failed			
	Failed Connection Attempts to 107.167.16.11	Failed Connection Attempts	Low	25,875	5,175					
	Failed Connection Attempts to 2.2.2.2	Failed Connection Attempts	Medium	25,640	5,128		Falled			Failed
	Failed Connection Attempts to 208.91.113.186	Failed Connection Attempts	Low	22,520	4,504		Failed Co			
	A Your.Freedom	Proxy	High	18,170	457			blocked-connection	Proxy.HTTF	Dist.
	Failed Connection Attempts to 12.12.12.123	Failed Connection Attempts	Medium	18,070	3,614		Failed	*		Falled
	Failed Connection Attempts to 216.239.38.10	Failed Connection Attempts	Low	17,965	3,593		Failed Co	Threat	blocked-connection	
	Failed Connection Attempts to 208.91.113.240	Failed Connection Attempts	Low	17,890	3,578		Falled	Category	Blocked by Firewall Policy	Falled
	Failed Connection Attempts to 172.16.106.128	Failed Connection Attempts	Medium	16,685	3,337			Threat Level	Critical	



13

Filter Data in FortiView



Use this drop-down menu to switch between different formats.

14



Drill Down and View Log Details

Here is the drill-down view of threat ow.ly at log level.



16

17



FortiAnalyzer provides a comprehensive set of easily customizable report templates for you to quickly build reports.

Predefined Report Templates

1. Go to Reports > Report Definitions > Templates to view the predefined report templates.

Reports 🗸				ADOM	1: root	오 admin 🗸 🌾
Report Definitions	~	+	🕻 Create New 🗹 Edit 🏦 Delete 📲 Clone			Q
All Reports	- 1		Title	Description	Category	▲ Preview
🗇 Templates			ForTemplate - 360-Degree Security Review	Security review of Application Visibility and Control, Threat Detection, Data Exfiltration Detection, Endpoint Detection, Prevention and Recommended Actions.	Security	HTML PDF
Macro Library			Template - Admin and System Events Report	Admin login and failed login attempts and system severity event counts.	System	HTML PDF
te Datasets	_		Formplate - Application Risk and Control	Application risk, categories, bandwidth by app, web categories,	Application	HTML PDF
Advanced Gotput Profile	~			vulnerability exploits, virus, botnet, adware malicious attacks, file transfers.		
A Language			Template - Bandwidth and Applications Report	Traffic, Bandwidth, Sessions, Destinations summaries - by users and applications	Application	HTML PDF
Report Calendar			Template - Client Reputation	Client and user network behaviour, incidents by user, devices, threat summary.	User	HTML PDF
			Template - Data Loss Prevention Detailed Report	Violation Summary and Activity Details of Email, Web, and FTP.	Security	HTML PDF
			For Template - Detailed Application Usage and Risk	Application Risk - botnet, proxy avoidance, peer-to-peer, remote access, email. Backup and storage, general access. Includes risk category examples.	Application	HTML PDF
			Template - Email Report	Email Senders and Recipients by Total Number and Size of emails.	Security	HTML PDF
			Formplate - FortiClient Default Report	Summaries for Installation, OS, Device, FCT version and client summary. Threat summary by AV threats, infected devices, detections, WF violations, AP firewall, errors and alerts, total threats found.	Security	HTML PDF
			Template - FortiClient Vulnerability Scan Report	The vulnerabilities detected through Forticlient scans across the network	Security	HTML PDF
			Template - Hourly Website Hits	Hourly Website Hits	Web	HTML PDF
			Template - IPS Report	Intrusions detected by type, severity, victims, sources, blocked, monitored, attacks over http-https.	Security	HTML PDF
			ForTemplate - PCI-DSS Compliance Review	Summaries for PCI DSS Compliance and Regulatory Requirements, Related Best Security Practices, PCI DSS 3.1 Regulation Details.	Security	HTML PDF
			For Template - Security Analysis	Security Analysis of traffic, application, user, destination, bandwidth and sessions. DHCP, Wifi, traffic history. Web usage by users, categories and sites. Top email by senders, recipients. Malware, botnet, intrusion detections, victims and sources. VPN usage. Admin Login and system events.	Security	HTML PDF
			Template - Threat Report	Malware, Botnets - detected, victims and sources. Intrusions detected, sources, blocked severity and timeline.	Security	HTML PDF
			Template - Top 20 Categories and Applications (Session)	Top 20 Categories and Applications (Session)	Application	HTML PDF
			For Template - Top 20 Category and Websites (Bandwidth)	Top 20 Category and Websites (Bandwidth)	Web	HTML PDF
			Template - Top 20 Category and Websites (Session)	Top 20 Category and Websites (Session)	Web	HTML PDF
			Template - Top 500 Sessions by Bandwidth	Top 500 Sessions by Bandwidth	Web	HTML PDF
			Template - Top Allowed and Blocked with Timestamps	Top Allowed Applications by Session and Top Blocked Applications by Bandwidth with Timestamps	Application	HTML PDF
			Template - User Detailed Browsing Log	Detailed Web Browsing Log by Users	User	HTMLPDF

2. Click HTML or PDF in the preview column to view the sample report.

Generate Reports

- Go to Reports > Report Definitions > All Reports. 1.
- Double click the Application Risk and Control Report. 2.
- 3. Click Run Report from the view report tab.
- Once the report is generated, click on a format link to view and/or download it. 4.

Reports 🗸						AD	OM: root	Q admin 🗸 🐵
Report Definitions	~		Settings Layout				Edit: App	lication Risk and Control
🖹 All Reports		🕑 Run F	Report 🛱 Delete					
Templates		Report I	Name		Format	Time Range	Status	
ul Chart Library		Appli	cation Risk and Contro	1-2016-09-14-1140	HTML PDF XML CSV	2016/09/07 00:00-2016/09/13 23:59	3s	
Macro Library								
E Datasets								
Advanced	*							
E Output Profile								
🍽 Language								
Report Calendar								
					Return			



Monitor Events

Configure Event Handler

Events are triggered when the values of certain log fields meet the criteria defined in the Event Handlers. To create an event handler to catch the Botnet events:

- Go to Event Management > Event Handler Lists. 1.
- Select the default handler: UTM App Ctrl Event. 2.
- 3. Click Clone.

Event Management 🗸					ADOM: ro	ot 요a	dmin 🗸 🍵
All Events	+	- Create New 🗹 Edit 🏢	Delete 🎦 Clone 🚦 More 🗸				Q
🖽 Calendar View		A Name	Filters	Event Type	Devices	Severity	Send Alert to
= Event Handler List		Antivirus Event	> 2 Filters	iii AntiVirus	All Devices	Medium	
		App Ctrl Event	> 2 Filters	Application Control	All Devices	Critical	
		Interface Up	> 2 Filters	i Event	All Devices	Medium	
		IPS - Critical Severity	Severity Equal To Critical	IPS IPS	All Devices	Critical	
	2	UTM App Ctrl Event	> 2 Filters	Application Control	All Devices	Critical	



- 4. Enter a custom name.
- 5. Remove the application category **Proxy** from the matching criteria.
- 6. Click **OK** to save the handler.

Clone Handler: UTM App Cl	rl Event									
Status	ON									
Name	Botnet App Ctrl Event									
Description	Botnet Application Control event handler									
Devices	● All Devices 〇 Specify 〇 Local Device									
Severity	Critical v									
Filters										
Log Type	Application Control *									
Group By	Application Name									
Logs match	O All Any of the following conditions									
Log Field	Match Criteria Value									
Application Category	• Equal To • Botnet • + 🖻									
Generic Text Filter 🔗										
Notifications										
Generate alert when at least	1 matches occurred over a period of 30 minutes									
Send Alert Email										
То	security@company.com									
From	admin@company.com									
Subject	Corporate_FGT									
Email Server	Corporate: smtp.company.com									
Send SNMP(v1/v2) Trap										
Send SNMP(v3) Trap	Please select v									
	Factory Reset OK Cancel									

View Events

All triggered events are displayed on the event list page. To view events:

- 1. Go to Event Management > All Events.
- 2. Click an entry from the list to view more details.

ver	nts by Ty	pe			Even	its by Severity		
					3		_	
		7.6%			2	5-		
		12.1%			2			
		34.8%	Traffic	(21)				
		Traffic	IPS (9		-18	5-		
		Events 21	Applic Other	ation Control (Types (5)	8) 10) -		
		Counts 149						
		31.8%				Critical	High	Medium Low
Rec	ent Ever	its (62) Show Acknowledged	Count	Councilla	Event Tune	T I ant I ladate	Manuffer	Additional lafe
	1	EVENT Name	1	Medium	Event type	* Last Opdate	Local Davice Event	Hogrado imago from vE 4 0-bui
	2	EAZ-VM0000005564	1	Medium	Event Event	2010-07-14 10:53:38	Local Device Event	Upgrade image from vE 4.0 but
	3	Asprov Botnet	1	Critical	Application Control	2016-09-13 15:35:44	Ann Ctrl Event	Botnet
	4	Asprox Botnet	1	Critical	Application Control	2016-09-13 15:35:29	LITM Ann Ctri Event	Botnet
	5	Asprox Botnet	1	Critical	Application Control	2016-09-13 15:35:29	UTM Ann Ctrl Event	Botnet
	6	Asprox Botnet	1	Critical	Application Control	2016-09-13 15:35:08	LITM Ann Ctrl Event	Botnet
	7	testing	6	Low	O Traffic	2016-09-13 15:34:42	testing	boulet
0	8	testing	2	Low	Ø Traffic	2016-09-13 15:34:26	testing	
0	9	testing	2	Low	C Traffic	2016-09-13 15:31:40	testing	
	10	testing	11	Low	✿ Traffic	2016-09-13 15:31:39	testing	
	11	KProxy	1	Critical	Application Control	2016-09-13 15:31:09	UTM App Ctrl Event	Proxy
	12	testing	2	Low	✿ Traffic	2016-09-13 15:29:11	testing	
	13	testing	2	Medium	© Traffic	2016-09-13 15:28:24	testing	
	14	testing	1	Medium	C Traffic	2016-09-13 15:27:48	testing	
	15	testing	10	Medium	Traffic	2016-09-13 15:27:27	testing	
	16	testing	4	Medium	Traffic	2016-09-13 15:27:22	testing	
	17	testing	2	Medium	Traffic	2016-09-13 15:26:10	testing	
	18	testing	49	Medium	Traffic	2016-09-13 15:24:32	testing	
	19	testing	4	Medium	Traffic	2016-09-13 15:24:06	testing	
	20	testing	18	Medium	Traffic	2016-09-13 15:23:40	testing	
	21	Somery.Include.PHP.File.Inclusion	2	High	IPS 1	2016-09-13 15:21:44	IPS - High Severity	Code Injection (CVE-2006-466
	22	Linksnet.Newsfeed.PHP.File.Inclusion	2	High	IPS 1	2016-09-13 15:21:15	IPS - High Severity	Code Injection (CVE-2007-270
	23	IISadmin.ISM.DLL.Access	1	High	IPS IPS	2016-09-13 15:21:14	IPS - High Severity	Information Disclosure (CVE-19
	24	GameSiteScript.Index.PHP.SQL.Injection	1	High	IPS	2016-09-13 15:21:01	IPS - High Severity	SQL Injection (CVE-2007-3631
0	25	LaVague.PrintBar.PHP.File.Inclusion	1	High	IPS	2016-09-13 15:20:44	IPS - High Severity	Code Injection (CVE-2007-260
	26	testing	4	Medium	Traffic	2016-09-13 15:20:39	testing	
	27	OTE.Header.PHP.File.Inclusion	1	High	IPS	2016-09-13 15:20:39	IPS - High Severity	Code Injection (CVE-2007-267
	28	OTE.Header.PHP.File.Inclusion	1	High	IPS IPS	2016-09-13 15:20:27	IPS - High Severity	Code Injection (CVE-2007-267
	29	Linksnet.Newsfeed.PHP.File.Inclusion	1	High	IPS 1	2016-09-13 15:20:08	IPS - High Severity	Code Injection (CVE-2007-270
	30	EICAR_TEST_FILE	3	High	i∰ AntiVirus	2016-09-13 15:15:35	UTM Antivirus Event	Virus (FortiGuard ID: 2172)
	31	Adware/TEST_FILE	1	High	₩ AntiVirus	2016-09-13 15:10:32	UTM Antivirus Event	Adware (FortiGuard ID: 2769)
	32	W32/NGVCK	2	High	★ AntiVirus	2016-09-13 15:10:31	UTM Antivirus Event	Virus (FortiGuard ID: 7602)



DAY 3: EXPLORE FURTHER

Enable Event Notification

You can send alert notifications via Email, SNMP, to Syslog Server.

To configure notifications:

Event Monitor > Event Handler List > [Event Handler] Edit

Create Custom Report

Create reports from predefined FortiAnalyzer templates, or use any of the 300+ predefined charts and 400+ datasets.

To create a custom report:

Reports > All Reports > Create New

Monitor Storage Usage Graphs

Monitor FortiAnalyzer disk space, data policy, storage and disk utilization, as well as drill down to Analytic and Archive usage by device.

To monitor storage usage:

Log View > Storage Statistics

System Dashboard Log Rate Widgets

Monitor logging rates and performance from the Dashboard. Useful widgets include **Insert Rate vs Receive Rate**, **Log Receive Monitor** and **Log Insert Lag Time**.

To add Widgets to monitor log rates:

System Settings > Dashboard > Toggle Widgets

Indicators of Compromise for APT Detection

FortiView > Threats > IOC



For more information, see <u>Administration Guide</u> and videos in <u>Fortinet Video Library</u>



LEARN MORE

FortiAnalyzer Administration Guide

http://docs.fortinet.com/fortianalyzer/admin-guides

Fortinet Document Library

http://docs.fortinet.com

Fortinet Video Guide

http://video.fortinet.com

Fortigate Cookbook

http://cookbook.fortinet.com

Training Services

http://www.fortinet.com/training

SUPPORT AND FEEDBACK

Customer Service & Support https://support.fortinet.com

Feedback on Fortinet technical document Email: techdocs@fortinet.com

FORTINET.COM